Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

OPERAZIONI ESTERNE

Tesi di Laurea in
Algebra

Relatore:
Chiar.mo Prof.
LIBERO VERARDI

Presentata da:
FEDERICA VERONESI

I Sessione
19 Giugno 2015

La gente pensa di non capire la matematica, ma tutto sta nel modo in cui la si spiega.
se chiediamo a un beone quale numero sia maggiore tra 2/3 e 3/5, non ce lo saprà dire.
Ma se riformuliamo la domanda: che cos'è meglio,
dividere due bottiglie di vodka fra tre persone,
o tre bottiglie fra cinque persone, vi dirà subito:
due bittiglie in tre, ovviamente.
Izrail' Gel'fand

Indice

Introduzione **III**

1 Richiami di algebra **1**

1.1 Le potenze 1

1.2 Gli spazi vettoriali 4

1.3 Gli A-moduli 5

1.4 Il coniugio 6

1.5 La congruenza di figure piane 8

2 Le operazioni esterne **13**

2.1 Definizioni iniziali 13

2.2 Nozioni generali applicate alle operazioni esterne 14

2.3 Condizioni di compatibilità 17

3 Esempi **19**

3.1 Azione di un gruppo su un insieme 19

3.1.1 L'azione del gruppo Γ delle isometrie sul piano euclideo 21

3.2 Azione di un anello su un gruppo abeliano 23

3.3 Le azioni di un gruppo su se stesso 27

3.3.1 Il coniugio 27

3.3.2 La moltiplicazione a sinistra 29

Conclusioni **33**

Bibliografia **35**

Ringraziamenti **37**

Introduzione

L'obiettivo principale di questo elaborato è di analizzare alcune situazioni algebrico-geometriche studiate nei corsi di algebra e geometria del Corso di Laurea triennale in Matematica, al fine di ricercare una nozione comune che possa generalizzare e unificare questi concetti. Tale nozione è quella di operazione esterna.

Nel primo capitolo abbiamo riproposto alcuni concetti già studiati. Abbiamo visto la definizione di potenza con esponente intero, le relative proprietà e il teorema che descrive il legame tra periodo di un elemento e le sue potenze. Inoltre abbiamo richiamato gli spazi vettoriali e la loro generalizzazione degli A-moduli, sottolineando le loro differenze: mentre per i primi esiste la nozione di base e quindi di dimensione, vale la legge di cancellazione; per i secondi non si possono definire le basi e non vale la legge di cancellazione. Si è poi definito il coniugio, parlando della relazione di essere coniugati e delle sue proprietà. Infine abbiamo studiato le isometrie del piano classificate in isometrie dirette (traslazioni e rotazioni) e indirette (simmetrie assiali e antitraslazioni).

Nel secondo capitolo abbiamo definito le operazioni esterne destre e sinistre, applicazioni definite su $\Omega \times X$ a valori in X, dove Ω e X sono insiemi non necessariamente coincidenti. Abbiamo definito la loro rappresentazione e il comportamento di un'azione trasferita all'insieme delle parti $\mathcal{P}(X)$. Abbiamo quindi descritto le nozioni associate alle azioni: gli Ω-sottoinsiemi, le Ω-congruenze e gli Ω-omomorfismi. Quindi abbiamo dimostrato il teorema fondamentale di omomorfismo. Infine abbiamo descritto le condizioni di compatibilità a cui deve soddisfare un'applicazione per essere un'azione quando su Ω o su X sia presente una qualsiasi struttura algebrica.

Nel terzo capitolo, utilizzando le nozioni introdotte nel precedente capitolo, si è cercato di comprendere che cosa avessero in comune le situazioni algebrico-geometriche viste nel primo capitolo. Abbiamo quindi descritto vari esempi concentrandoci in particolar

modo sulle condizioni di compatibilità e sulle nozioni generali riguardo le azioni esterne che ivi acquistano un significato particolare.

Capitolo 1

Richiami di algebra

In questo primo capitolo si richiamano alcuni concetti apparentemente alla rinfusa e slegati tra loro, tratti dai corsi di algebra dei primi due anni della Triennale (si veda [1] e [2]). Successivamente si vedrà che cosa hanno in comune.

1.1 Le potenze

Definizione 1.1. Sia $(G, \cdot)$ un gruppo e sia $x \in G$, sia x' il suo simmetrico cioè tale che $x \cdot x' = 1$. Si possono definire le *potenze con esponente intero* in questo modo:

$$\begin{cases} x^0 = 1_G \\ x^{n+1} = x^n \cdot x \qquad \forall n \in \mathbb{N}, \quad n > 0 \\ x^{-n} = x'^n \end{cases}$$

Proposizione 1.1.1. *Sia $(G, \cdot)$ un gruppo e siano $x, y \in G$, $m, n \in \mathbb{Z}$. Valgono le seguenti proprietà:*

1. $x^m \cdot x^n = x^{m+n}$
2. $(x^m)^n = x^{m \cdot n}$
3. *Se $x \cdot y = y \cdot x$ allora $\forall n \in \mathbb{Z}$, $(x \cdot y)^n = x^n \cdot y^n$.*
   Viceversa se $(x \cdot y)^2 = x^2 \cdot y^2$ si ha $x \cdot y = y \cdot x$ quindi
   $(x \cdot y)^n = x^n \cdot y^n, \quad \forall n \in \mathbb{Z}$.

Dimostrazione. 1. Sia $n \geq 0$, uso il principio di induzione per dimostrare la prima proprietà. Se $n = 0$ si ha

$$x^m \cdot x^0 = x^m \cdot 1_G = x^m$$

$$x^{m+0} = x^m$$

quindi la proprietà 1) vale per $n = 0$. Ora supponiamo che sia verificata per n e proviamola per $n + 1$:
$x^m \cdot x^{n+1} = x^m \cdot (x^n \cdot x) = (x^m \cdot x^n) \cdot x = x^{m+n} \cdot x = x^{(m+n)+1} = x^{m+(n+1)}$
quindi la proprietà è verificata $\forall m, n \in \mathbb{Z}, \quad n \geq 0$.
In particolare si ha

$$x^{-n} \cdot x^n = x^{-n+n} = x^0 = 1_G \Rightarrow \begin{cases} x^{-n} = (x^n)^{-1} \\ x^n = (x^{-n})^{-1} \end{cases}$$

Grazie a quest'ultima osservazione, si può dimostrare che $\forall n \in \mathbb{N}$ vale
$x^m \cdot x^{-n} = x^{m+(-n)}$, distinguiamo però due casi:

a) Se $m < 0$ allora $m' = -m > 0$ quindi

$$\begin{aligned} x^m \cdot x^{-n} = (x^{-1})^{m'} \cdot (x^{-1})^n = (x^{-1})^{m'+n} = \\ = x^{-(m'+n)} = x^{-m'-n} = x^{m-n} = x^{m+(-n)} \end{aligned}$$

b) Se $m > 0$, pongo $x' = x^{-1}$ allora si ha

$$x^m = (x^{-m})^{-1} = (x'^m)^{-1} = x'^{-m}$$

dato che $x^{-n} = x'^n$ si ha anche

$$x^m \cdot x^{-n} = x'^{-m} x \cdot x'^n = x'^{-m+n} = x'^{-(m-n)} = x^{m+(-n)}$$

2. Per il principio induzione $\forall m, n \in \mathbb{Z}, \quad n \geq 0$ si ha che se $n = 0$

$$(x^m)^0 = 1_G$$

$$x^{m \cdot 0} = x^0 = 1_G$$

Supponiamo che la proprietà sia verificata per n e si vuole dimostrarla per $n + 1$:

$$(x^m)^{n+1} = (x^m)^n \cdot x^m = x^{m \cdot n} \cdot x^m = x^{m \cdot n + m} = x^{m(n+1)}$$

Inoltre $(x^m)^{-n} = ((x^m)^{-1})^n = (x^{-m})^n = x^{(-m) \cdot n}$

3. Sia $n \geq 0$, si ragiona ancora per induzione: per $n = 0$ si ha

$$(x \cdot y)^0 = 1_G = (y \cdot x)^0$$

Supponiamo che la proprietà sia vera per n e dimostriamo per $n+1$:

$$(x \cdot y)^{n+1} = (x \cdot y)^n (x \cdot y) = x^n \cdot y^n \cdot x \cdot y = (x^n \cdot x)(y^n \cdot y) = x^{n+1} \cdot y^{n+1}$$

Inoltre vale:

$$(xy)^{-n} = ((xy)^n)^{-1} = (x^n y^n)^{-1} = x^{-n} y^{-n}$$

Inversamente, se $(x \cdot y)^2 = x^2 \cdot y^2$ allora, per la legge di cancellazione, si ha

$$xy \cdot xy = x \cdot x \cdot y \cdot y$$
$$y \cdot x = x \cdot y$$

quindi per quanto detto precedentemente si ha $(xy)^n = x^n y^n, \quad \forall n \in \mathbb{Z}$

□

Infine possiamo descrivere la relazione tra il numero di potenze distinte e il minimo esponente per cui si ottiene l'elemento neutro.

Definizione 1.2. Si definisce *periodo*, o ordine, di un elemento $x \in G$ il numero di potenze distinte di x, cioè il minimo degli interi k tali che $x^k = 1_G$.

Teorema 1.1.2. *Siano G un gruppo e $x \in G$. Allora*

1. *il periodo di x è infinito se e solo se $\forall m, n \in \mathbb{Z}, \quad m \neq n \Rightarrow x^n \neq x^m$;*
2. *se $|x| = n$ allora $n = min\left\{h \in \mathbb{N} | h > 0, x^h = 1_G\right\}$ quindi si ha che l'insieme delle potenze a esponente intero di x è $\langle x \rangle = \{x^0, x^1, ..., x^{n-1}\}$;*
3. *se $|x| = n$, si ha $x^k = 1_G \Leftrightarrow k \quad divide \quad n$.*

Dimostrazione. 1. Per dimostrare la prima affermazione bisogna provare le due implicazioni:

- $\Leftarrow$ Supponiamo che $\forall n, m \in \mathbb{Z}, \quad m \neq n \Rightarrow x^n \neq x^m$ e consideriamo la funzione $f \colon \mathbb{Z} \to \langle x \rangle, \quad f(n) = x^n$. Tale funzione è ben definita e biiettiva quindi x ha periodo infinito.
- $\Rightarrow$ Viceversa, se $x^n = x^n$, sia per esempio $n > m$, allora $x^{n-m} = 1_G$.
  Per il lemma di divisione euclideo, sappiamo che $\forall k \in \mathbb{Z}, \quad \exists q, r$ tali che $k = (n-m)q + r$ con $0 \leq r < n - m$ quindi si ottiene:

  $$x^k = x^{(n-m)q+r} = x^{(n-m)q} \cdot x^r = (x^{n-m})^q \cdot x^r = 1_G x^r = x^r$$

  dove $x^r \in \left\{x^0, x^1, ..., x^{(n-m)-1}\right\}$
  Quindi $\langle x \rangle \subseteq \left\{x^0, x^1, ..., x^{(n-m)-1}\right\}$
  Inoltre vale anche l'inclusione opposta quindi i due insieme coincidono. Allora $\langle x \rangle$ è finito.

2. Per il primo punto di questo teorema, poiché x ha ordine finito, sappiamo che le potenze di x non sono tutte distinte quindi esistono $h \in \mathbb{Z}, \quad h > 0$ tali che $x^h = 1_G$. Sia m il minimo di questi esponenti, allora si ottiene $\langle x \rangle = \{x^0, x^1, ..., x^{m-1}\}$.
Inoltre se $0 < h < k < m$ allora deve essere $x^h \neq x^k$ altrimenti sarebbe $x^{k-h} = 1_G$ con $0 < k - h < m$, ma ciò è assurdo poiché m è il minimo degli esponenti per i quali si ottiene 1_G.
Quindi $n = |\langle x| \rangle = |\{x^0, x^1, ..., x^{m-1}\}| = m$

3. Supponiamo $|x| = n$, si pone $k = nq + r$ dove $0 \leq r < n$ quindi $1_G = x^k = x^r$ dunque deve essere $r = 0$ dato che n è il minimo. Allora $n|k$

□

1.2 Gli spazi vettoriali

Definizione 1.3. Siano K un campo. Un *K-spazio vettoriale* V è un insieme su cui sono definite due operazioni: una somma ($+ \colon V \times V \longrightarrow V$) e un prodotto per scalari ($\cdot \colon K \times V \longrightarrow V$) che soddisfano le seguenti proprietà:

i) $\forall h, k \in K, \ \forall v \in V$

$$(h + k) \cdot v = h \cdot v + k \cdot v$$
$$(hk) \cdot v = h \cdot (k \cdot v)$$

ii) $\forall k \in K, \ \forall v, w \in V$

$$k \cdot (v + w) = k \cdot v + k \cdot w$$

iii) $1_K \cdot v = v$

Definizione 1.4. Un *sottospazio vettoriale* di uno spazio vettoriale V è un sottoinsieme $W \subseteq V$ chiuso rispetto alla somma e al prodotto per scalari, cioè

$$\forall v, w \in W, \forall k \in K, \quad \text{si ha} \quad v + w \in W, \quad k * v \in W$$

Definizione 1.5. Dato uno spazio vettoriale V, si chiama *base* dello spazio, un insieme $\{v_1, ..., v_n\}$ di elementi di V tali che:

i) $v_1, ..., v_n$ sono un insieme di generatori di V cioè $V = Span\{v_1, ..., v_n\}$;

ii) $v_1, ..., v_n$ sono linearmente indipendenti.

Inoltre si chiama *dimensione* dello spazio V la cardinalità di una qualunque sua base. In particolare, lo spazio vettoriale $\{0\}$ composto dal solo vettore nullo ha dimensione zero mentre uno spazio vettoriale che non ha sistemi di generatori finiti, ha dimensione infinita.

Osservazione. In uno spazio vettoriale V vale la legge di annullamento del prodotto: $\forall k \in K$, $\forall v \in V$,

$$k \cdot v = 0_V \Leftrightarrow k = 0_K \text{ oppure } v = 0_V$$

Vale inoltre la legge di cancellazione: $\forall u, v, w \in V$ si ha

$$u \cdot v = u \cdot w \;\Rightarrow\; v = w$$
$$v \cdot u = w \cdot u \;\Rightarrow\; v = w$$

1.3 Gli A-moduli

Analogamente a quanto detto per gli spazi vettoriali, possiamo ora definire la struttura di modulo su un anello.

Definizione 1.6. Sia $(A, +, \cdot, 1_A)$ un anello commutativo. Un *A-modulo* è un insieme M dotato di due operazioni: la somma $+\colon M \times M \longrightarrow M$ e il prodotto per uno scalare $\cdot\colon A \times M \longrightarrow M$, tale che soddifsfa le proprietà della definizione 1.3 di spazio vettoriale.

Definizione 1.7. Sia M un A-modulo. Un sottoinsieme $\emptyset \neq N \subseteq M$ è detto *sottomodulo* se:

i) N è un sottogruppo abeliano di M;

ii) $\forall a \in A, \quad \forall n \in N$ si ha $an \in N$.

Definizione 1.8. Un'applicazione tra A-moduli, $f\colon M \to N$, si dice *A-omomorfismo* se mantiene la struttura di modulo cioè è tale che:

i) $f(m + m') = f(m) + f(m')$

ii) $f(a \cdot m) = a \cdot f(m)$

$\forall a \in A, \quad \forall m, m' \in M$.

Proposizione 1.3.1. *Sia $f\colon M \to N$ un A-omomorfismo. Allora l'immagine*

$$Imf = f(M) = \{n \in N : n = f(m) \quad \forall m \in M\}$$

e il nucleo

$$Kerf = \{m \in M : f(m) = 0\}$$

sono sottomoduli rispettivamente di N e di M. In particolare f è un omomorfismo suriettivo se e solo se $Imf = N$ e iniettivo se e solo se $Kerf = \{0\}$.

Dimostrazione. Vogliamo provare che Imf è sottomodulo di N: sappiamo dalla teoria dei gruppi che Imf è sottogruppo del gruppo $(N, +)$; inoltre

$$\forall a \in A, \quad \forall n \in Imf \quad \text{esiste} \quad m \in M \quad \text{tale che} \quad a \cdot n = a \cdot f(m) = f(am)$$

Poiché $am \in M, \quad \forall a \in A, \quad \forall m \in M$ si ha $an \in N$.
Analogamente si può dimostrare che $Kerf$ è un sottomodulo di M: ancora dalla teoria dei gruppi sappiamo che $Kerf$ è sottogruppo di $(M, +)$; inoltre

$$\forall a \in A, \quad \forall m \in Kerf \quad \text{si ha} \quad f(a \cdot m) = a \cdot f(m) = a \cdot 0 = 0$$

Quindi $am \in Kerf$.
Infine f è un omomorfismo iniettivo se e solo se $Kerf = \{0\}$ infatti se f è iniettivo, si considera $m \in Kerf$ e si ha $f(m) = 0 = f(0)$ perciò $m = 0$.
Viceversa se $Kerf = \{0\}$, si considera $f(m) = f(n)$ con $m, n \in M$ allora $0 = f(m) - f(n) = f(m - n)$ quindi $m - n \in Kerf$ cioè $m - n = 0$. Si ottiene $m = n$ quindi f iniettivo. □

1.4 Il coniugio

Dato un gruppo G e un suo elemento $a \in G$, definiamo l'applicazione

$$\begin{aligned} C_a \colon G &\longrightarrow G \\ x &\longmapsto axa^{-1} \end{aligned}$$

e vediamo alcune delle sue principali caratteristiche:

Proposizione 1.4.1. *1. Siano $a, b, x, y \in G$ allora*

a) $C_1(x) = x$;

b) $C_a(xy) = C_a(x)C_a(y)$;

c) $C_{ab}(x) = C_a(C_b(x))$.

2. La funzione C_a è un isomorfismo di gruppi. Inoltre

a) C_1 è l'identità;

b) $C_{a^{-1}} = (C_a)^{-1}$;

c) se $a, b \in G$ allora $C_{ab} = C_a C_b$.

Dimostrazione. 1. $C_1(x) = 1x1^{-1} = x$
$C_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = C_a(x)C_a(y)$
$C_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(C_b(x))a^{-1} = C_a(C_b(x))$

2. La prima parte della dimostrazione ci dice che C_1 è l'identità, che C_a è un omomorfismo di gruppi e che $C_{ab} = C_a C_b$. Inoltre $C_a C_{a^{-1}} = C_{aa^{-1}} = C_1$ quindi $C_{a^{-1}} = (C_a)^{-1}$. Allora si ha che C_a è biunivoca perciò è un isomorfismo.

□

Definizione 1.9. Sia G un gruppo e siano $x, y \in G$. Si dice che x *è coniugato a* y se esiste $a \in G$ tale che $y = C_a(x) = axa^{-1}$.

La relazione di coniugio è una relazione di equivalenza. Infatti valgono le proprietà:

- riflessiva: $x = 1x1^{-1}$;
- simmetrica: $x = aya^{-1} \Rightarrow a^{-1}xa = (a^{-1})x(a^{-1})^{-1} = y$;
- transitiva: $x = aya^{-1}$ e $y = bzb^{-1} \Rightarrow x = abzb^{-1}a^{-1} = (ab)z(ab)^{-1}$.

Si può quindi definire la *classe di coniugio* di un qualsiasi elemento $a \in G$:

$$[a] = \left\{gag^{-1} : g \in G\right\}$$

Osservazione. Se G è un gruppo abeliano allora per ogni $a \in G$ si ha $[a] = \{a\}$.

Basta infatti osservare che in un gruppo abeliano vale la proprietà commutativa quindi $[a] = \{gag^{-1} : g \in G\} = \{agg^{-1} : g \in G\} = \{a\}$

Proposizione 1.4.2. *Sia G un gruppo, allora valgono:*

1. *l'unità è coniugata solo a se stessa;*
2. *Se $a, b \in G$ sono coniugati allora sono coniugate anche le loro potenze k-esime.*

Dimostrazione. 1. $[1_G] = \{g1_G g^{-1} : g \in G\} = \{1_G\}$ dato che $g1_G g^{-1} = gg^{-1} = 1_G$

2. se a, b sono coniugati significa che esiste $g \in G$ tale che $a = gbg^{-1}$. Allora elevando alla potenza k-esima si ottiene:

$$a^k = (gbg^{-1})^k = gb^k g^{-1}$$

quindi a^k, b^k sono coniugati.

□

Proposizione 1.4.3. *Sia G un gruppo allora*

1. *due elementi $a, b \in G$ sono coniugati solo se hanno lo stesso ordine;*[1]

[1] La condizione è solo necessaria infatti non sempre elementi con lo stesso ordine, sono anche coniugati. Per esempio in S_4 gli elementi $\alpha = (12)$, $\beta = (12)(34)$ hanno entrambi ordine 2 ma non sono coniugati.

2. *il numero di elementi coniugati ad* $a \in G$ *è pari a* $[G : Z(a)]$, *dove* $Z(a) = \{g \in G : ga = ag\}$ *è il sottogruppo di* G *detto centralizzante di* a;

3. $a \in Z(G) \Leftrightarrow [a] = \{a\}$ *dove* $Z(G) = \{x : gx = xg \quad \forall g \in G\}$ *è il centro di* G.

Dimostrazione. 1. Se $a, b \in G$ sono coniugati significa che $\exists g \in G : a = gbg^{-1}$. Supponiamo che a abbia ordine n, cioè $a^n = 1_G$ allora $(gbg^{-1})^n = 1_G$ cioè $gb^n g^{-1} = 1_G \Rightarrow b^n = 1_G$; allora anche b ha ordine n.
Viceversa se b ha ordine n cioè $b^n = 1_G$ allora $a^n = (gbg^{-1})^n = gb^n g^{-1} = 1_G$.
Quindi $a^n = 1_G \Leftrightarrow b^n = 1_G$

2. Sia $a \in G$ e consideriamo due suoi elementi coniugati: gag^{-1}, hah^{-1} dove $h, g \in G$. Affinché si abbia $gag^{-1} = hah^{-1}$ si deve avere $h^{-1}gag^{-1}h = a$ cioè $(h^{-1}g)a(h^{-1}g)^{-1} = a$.
Allora $h^{-1}g$ commuta con a cioè sta nel centralizzante $Z(a)$ allora g, h coniugano a allo stesso elemento se e solo se sono congruenti modulo $Z(a)$, se e solo se appartengono allo stesso laterale destro di $Z(a)$. Allora c'è un coniugato di a per ogni laterale destro di $Z(a)$ quindi, per il noto teorema di Lagrange, i coniugati di a sono proprio $[G : Z(a)]$.

3. la terza affermazione segue dal risultato precedente.

□

1.5 La congruenza di figure piane

Due figure piane di dicono congruenti quando esiste un'isometria che trasforma l'una nell'altra. In questa sezione vogliamo descrivere il gruppo non abeliano delle isometrie piane.

Definizione 1.10. Sia $\mathcal{P}$ l'insieme dei punti del piano. Si chiama *isometria del piano* una biiezione $f \colon \mathcal{P} \longrightarrow \mathcal{P}$ tale che $\forall P, Q \in \mathcal{P}$, posto $P' = f(P), Q' = f(Q)$, si ha $P'Q' \equiv PQ$.

In questa sezione indicheremo con il simbolo $\equiv$ l'uguaglianza in senso geometrico di figure piane.

Proposizione 1.5.1. *Chiamato* Γ *l'insieme delle isometrie del piano si ha che* Γ *è sottogruppo del gruppo simmetrico* $S_{\mathcal{P}}$ *delle biiezioni del piano* $\mathcal{P}$ *in sé.*

Dimostrazione. Di certo $id \in \Gamma$.
Siano $f, g \in \Gamma$ e $P, Q \in \mathcal{P}$; si pone $P' = f(P), \quad Q' = f(Q)$ e $P'' = f(P'), \quad Q'' = f(Q')$.
Allora, poiché f, g sono isometrie, si ottiene $P'Q' \equiv PQ$ e $P''Q'' \equiv P'Q'$ quindi $P''Q'' \equiv$

PQ. Ciò significa che anche $g \circ f$ è un'isometria, infatti trasforma P in P'' e Q in Q''. Infine è anche $PQ \equiv P'Q'$ quindi pure f^{-1} è un'isometria che porta P' in P e Q' in Q. □

Definizione 1.11. Siano $P \in \mathcal{P}$ un punto e s una retta del piano $\mathcal{P}$. Si definisce *simmetrico* di P rispetto a s il punto P' tale che la retta PP' sia perpendicolare alla retta s e il punto medio di PP' appartenga a s.

Definizione 1.12. Siano P un punto e s una retta del piano $\mathcal{P}$. Si chiama *simmetria assiale* rispetto a s la funzione σ che a ogni punto P associa il simmetrico P'.

Teorema 1.5.2. *Ogni isometria è esprimibile come prodotto di al più tre simmetrie assiali.*

Questo teorema dice che le simmetrie assiali sono un sistema di generatori per l'insieme G delle isometrie del piano. Per dimostrarlo occorrono i seguenti lemmi:

Lemma 1.5.3. *Siano A, B due punti distinti del piano. Esistono due e solo due isometrie che hanno A e B come punti fissi: l'identità e la simmetria σ rispetto alla retta AB.*

Lemma 1.5.4. *Dati due segmenti AB, $A'B'$ uguali e non degeneri, allora esistono due e solo due isometrie f_1, f_2 che portano A in A' e B in B'. Detta σ la simmetria rispetto alla retta $A'B'$ si ha $f_2 = \sigma \circ f_1$. Inoltre ciascuna delle due è prodotto di al più tre simmetrie.*

Lemma 1.5.5. *Dati due triangoli ABC e $A'B'C'$ non degeneri, con $AB \equiv A'B', BC \equiv B'C', AC \equiv A'C'$, esiste una ed una sola isometria che porta A in A', B in B', C in C' ed essa coincide con una delle due che portano A in A' e B in B'.*

Dimostrazione del teorema 1.5.2. Consideriamo un'isometria f e tre punti del piano, A, B, C, non allineati.
Poniamo $A' = f(A)$, $B' = f(B)$, $C' = f(B)$, allora per il lemma 1.5.5, f coincide con una delle due isometrie, siano f_1 e f_2, che portano rispettivamente A in A' e B in B'. Ora per il lemma 1.5.4, sappiamo che f_1 e f_2 sono prodotto di al più tre simmetrie, perciò il teorema è provato. □

Definizione 1.13. Siano s_1 e s_2 due rette del piano $\mathcal{P}$ e siano σ_1 e σ_2 le simmetrie assiali rispetto a tali rette. Considero un punto A del piano e chiamo r la retta passante per A e perpendicolare a s_1 e s_2.
Si chiama *traslazione* l'isometria $\tau = \sigma_2 \circ \sigma_1$ che associa al punto A il punto A' della retta r che si trova a distanza doppia rispetto a quella tra le rette s_1 e s_2. Inoltre a ogni traslazione è associato un vettore del piano $v = v(\tau)$.

Definizione 1.14. Siano s_1 e s_2 due rette del piano $\mathcal{P}$ e O il loro punto di intersezione; siano inoltre σ_1 e σ_2 le simmetrie assiali rispetto a tali rette. Si chiama *rotazione di centro O e ampiezza α* l'isometria che associa a ogni punto P il punto P' tale che $OP \equiv OP'$ e $\widehat{POP'} = \alpha$.

Se chiamiamo *movimenti del piano* l'insieme di traslazioni e rotazioni, vale il seguente teorema:

Teorema 1.5.6. *L'insieme M dei movimenti del piano costituisce un sottogruppo del gruppo Γ delle isometrie del piano.*

Dimostrazione. L'insieme T delle traslazioni è un sottogruppo del gruppo Γ delle isometrie piane. Infatti contiene l'identità dato che id è la traslazione associata al vettore nullo.
Ora consideriamo due punti $A, B \in \mathcal{P}$, la traslazione $\tau_1 \in T$ tale che $A' = \tau_1(A)$, $B' = \tau_2(B)$ a cui è associato il vettore $v_1 = v(\tau_1)$ rappresentato da $\vec{AA'}$ e $\vec{BB'}$; analogamente consideriamo la traslazione $\tau_2 \in T$ con $A'' = \tau_1(A')$, $B'' = \tau_2(B')$ a cui è associato il vettore $v_2 = v(\tau_2)$ rappresentato da $\vec{A'A''}$ e $\vec{B'B''}$. Poiché $AA'B'B$ e $A'A''B''B'$ sono parallelogrammi, allora $\vec{AB}$ e $\vec{A''B''}$ sono equipollenti. Si ha dunque che pure $AA''B''B$ è un parallelogramma, quindi l'isometria $\tau = \tau_2 \circ \tau_1$ è una traslazione, associata al vettore $v = \vec{AA''}$, che è uguale a $v_1 + v_2$.
Infine se consideriamo la traslazione $\tau \in T$, sappiamo che $\tau = \sigma_1 \circ \sigma_2$, dove σ_1 e σ_2 sono simmetrie assiali. Allora anche $\tau^{-1} = \sigma_2 \circ \sigma_1$ è una traslazione di vettore opposto.

In modo analogo si può dimostrare che l'insieme delle rotazioni di centro O è un sottogruppo di Γ. Tale insieme contiene l'identità che può essere pensata come la rotazione di centro O e ampiezza nulla.
Se ρ_1 e ρ_2 sono rotazioni di centro O ampiezza rispettivamente α_1 e α_2 allora la composizione $\rho = \rho_1 \circ \rho_2$ è ancora una rotazione di centro O e ampiezza $\alpha_1 + \alpha_2 \pmod{2\pi}$.
Infine l'inversa di una rotazione ρ di centro O e ampiezza α è la rotazione ρ^{-1} con stesso centro e ampiezza $2\pi - \alpha$.

Ora rimane da provare che la composizione di una traslazione e di una rotazione è un movimento. Sia $\rho = \sigma_2 \circ \sigma_1$ una rotazione di centro O e ampiezza α e sia $\tau = \sigma_4 \circ \sigma_3$ una traslazione, sia anche $\sigma_2 = \sigma_3$. Allora gli assi di simmetria s_1 e s_4 per σ_1 e σ_4 si incontrano nel punto O' e si ha $\tau \circ \rho = \sigma_4 \circ \sigma_3 \circ \sigma_2 \circ \sigma_1 = \sigma_4 \circ \sigma_1$ che è una rotazione di ampiezza α; questo risultato segue dal teorema sugli angoli alterni interni di rette parallele tagliate da una trasversale. Analogamente si prova che $\rho \circ \tau$ è una rotazione di ampiezza α. □

Si chiama *isometria inversa* qualunque isometria che non sia un movimento. Quindi sono isometrie inverse le simmetrie e i prodotti di tre simmetrie.

Definizione 1.15. Si dice *antitraslazione* il prodotto di una traslazione τ di vettore v con una simmetria σ di asse parallelo a v.

Teorema 1.5.7. *Le simmetrie inverse sono simmetrie assiali o antitraslazioni.*

Dimostrazione. Consideriamo tre simmetrie assiali σ_i di assi s_i, $i = \{1, 2, 3\}$. Se i tre assi sono paralleli o si incontrano nello stesso punto allora il prodotto è una simmetria. Nel primo caso si ha che il prodotto $\sigma_3 \circ \sigma_2$ è una traslazione che possiamo scrivere come prodotto di due simmetrie diverse, $\sigma_3' \circ \sigma_2'$, scegliendo $\sigma_2' = \sigma_1$. Allora si ottiene

$$(\sigma_3 \circ \sigma_2) \circ \sigma_1 = (\sigma_3' \circ \sigma_2') \circ \sigma_1 = \sigma_3 \circ (\sigma_2' \circ \sigma_1) = \sigma_3'$$

Nel secondo caso, si ragiona in modo analogo. Sia O il punto di intersezione dei tre assi, se compongo due simmetrie ottengo una rotazione di centro O che posso ottenere come prodotto della terza simmetria e un'altra diversa dalle σ_i. Il calcolo è analogo.

Ora supponiamo che gli assi s_2 e s_3 non siano paralleli allora $\sigma_3 \circ \sigma_2$ è una rotazione che si può rappresentare come prodotto di altre due simmetrie, $\sigma_3' \circ \sigma_2'$, di assi s_3 e s_2, scegliendo s_2' e s_1 perpendicolari. Allora sia $\rho = \sigma_2' \circ \sigma_1$, è una rotazione di ampiezza π quindi è una simmetria centrale di centro il punto di intersezione di s_1 e s_2'. POsso scrivere ρ come prodotto di altre due simmetrie, $\sigma_2'' \circ \sigma_1'$, di assi s_2'' e s_1' tali che s_1' e s_3' siano perpendicolari quindi $s_2'' // s_3'$. Alllora $\sigma_3' \circ \sigma_2'$ è una traslazione τ che ha vettore associato parallelo a s_1' cioè

$$\sigma_3 \circ \sigma_2 \circ \sigma_1 = (\sigma_3' \circ \sigma_2') \circ \sigma_1 = \tau \circ \sigma_1$$

quindi $\sigma_3 \circ \sigma_2 \circ \sigma_1$ è un'antitraslazione in quanto prodotto di una traslazione di vettore v e di una simmetria con asse parallelo a v.
Se s_2 e s_3 sono paralleli, ma non lo sono s_1 e s_2 allora si ragiona nello stesso modo. □

Abbiamo quindi definito i vari tipi di isometrie: simmetrie assiali, traslazioni, rotazioni e antitraslazioni, classificandole in movimenti e isometrie inverse.
Due figure piane $\mathfrak{F}_1$ e $\mathfrak{F}_2$ si dicono *isometriche* se esiste una isometria f tale che $F(\mathfrak{F}_1) = \mathfrak{F}_2$. In questo modo si ottiene una relazione di equivalenza nell'insieme delle figure piane, cioè dei sottoinsiemi di punti del piano, le cui classi di equivalenza sono dette *classi di isometria*. Per esempio la classe di isometria del quadrato è l'insieme dei quadrati con lati congruenti.
Inoltre per ogni figura $\mathfrak{F}$, possiamo considerare l'insieme $\{\alpha \in \Gamma | \alpha(\mathfrak{F}) = \mathfrak{F}\}$ che è sottogruppo di Γ detto *gruppo di simmetrie* di $\mathfrak{F}$.

Un Ω-sottoinsieme del piano $\mathcal{P}$ è unione di classi di isometria. Per esempio l'insieme dei poligoni è un Ω-sottoinsieme, come anche l'insieme dei punti, delle rette e delle coniche.

Capitolo 2

Le operazioni esterne

In questo capitolo si dà la definizione di operazione esterna e si introducono le nozioni ad essa legate. Infine analizziamo le condizioni di compatibilità tra azione e struttura algebrica avvicinandoci a comprendere cosa hanno in comune le situazioni algebrico-geometriche viste nel capitolo precedente.

2.1 Definizioni iniziali

Oltre alle operazioni binarie interne, nelle quali i termini e il risultato appartengono allo stesso insieme X, è possibile considerare operazioni esterne (destre o sinistre), nelle quali i termini appartengono a due insiemi Ω e X che non necessariamente coincidono.

Definizione 2.1. Un'*azione sinistra* di un insieme Ω su un insieme X è una legge

$$\begin{aligned} \mu\colon \Omega \times X &\longrightarrow X \\ (\omega, x) &\longmapsto \omega x \end{aligned}$$

In questo caso X è detto Ω-*insieme*.
Analogamente si definisce un'*azione destra*[1] come una legge

$$\begin{aligned} \mu\colon X \times \Omega &\longrightarrow X \\ (x, \omega) &\longmapsto x^{\omega} \end{aligned}$$

Definizione 2.2. Fissato $\omega \in \Omega$ si può considerare la funzione

$$\begin{aligned} \tau_{\omega}\colon X &\longrightarrow X \\ x &\longmapsto \omega x \end{aligned}$$

[1]Si osservi che per le azioni destre si usa la notazione esponenziale.

Si definisce quindi la *rappresentazione di* Ω come l'applicazione

$$\begin{aligned} \rho_\mu \colon \Omega &\longrightarrow X^X \\ \omega &\longmapsto \tau_\omega \end{aligned}$$

Definizione 2.3. Viceversa, data una funzione $\rho \colon \Omega \longrightarrow X^X$, posto $\forall \omega \in \Omega$, $\tau_\omega = \rho(\omega)$, si definisce la funzione

$$\begin{aligned} \mu \colon \Omega \times X &\longrightarrow X \\ (\omega, x) &\longmapsto \tau_\omega(x) \end{aligned}$$

Si ha che μ è un'azione sinistra di Ω su X.

Osservazione. L'azione di Ω su X si trasferisce a $\mathcal{P}(X)$ cioè diventa
$\mu \colon \Omega \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ e agisce in questo modo:

$$\forall \omega \in \Omega, \quad \forall Y \in \mathcal{P}(X) \quad \text{si ha} \quad \mu(\omega, Y) = wY = \{wy \quad | \quad y \in Y\}$$

2.2 Nozioni generali applicate alle operazioni esterne

Ora definiamo le principali nozioni associate alle operazione esterne. Consideriamo gli insiemi Ω, X e l'azione

$$\begin{aligned} \mu \colon \Omega \times X &\longrightarrow X \\ (\omega, x) &\longmapsto \omega x \end{aligned}$$

Definizione 2.4. Un sottoinsieme Y di X è detto Ω-*sottoinsieme* se $\forall \omega \in \Omega$, $\forall y \in Y$ si ha $\omega y \in Y$.

Teorema 2.2.1. *L'unione e l'intersezione di* Ω*-sottoinsiemi è ancora un* Ω*-sottoinsieme.*

Dimostrazione. Sia $\mathcal{L}_\Omega(X)$ l'insieme degli Ω-sottoinsiemi di X, sia $\mathcal{F} \in \mathcal{L}_\Omega(X)$ e si chiamino

$$A = \bigcap_{Y \subseteq \mathcal{F}} Y \quad \text{e} \quad B = \bigcup_{Y \subseteq \mathcal{F}} Y$$

Si vuole dimostrare che A e B sono ancora Ω-sottoinsiemi di X.
Sia $y \in A$ allora $\forall Y \subseteq A$, $y \in Y$ quindi $\forall \omega \in \Omega$ si ha $wy \in Y$ e dunque $wy \in A$.
Analogamente sia $y \in B$ allora esiste almeno un $Y \subseteq B$ tale che $y \in Y$; quindi $\forall \omega \in \Omega$ si ha $wy \in Y$ e quindi $wy \in B$. □

Definizione 2.5. Una relazione d'equivalenza $\sim$ in X si dice Ω-*congruenza* se $\forall x, y \in X$, $\forall \omega \in \Omega$, $x \sim y \Rightarrow \omega x \sim \omega y$.
A questo punto è facile definire l'Ω-insieme quoziente: l'azione si trasferisce al quoziente $X/\sim$ ponendo $\omega\,[x]_\sim = [\omega x]_\sim$

Tale definizione di insieme quoziente è ben posta infatti se $[x]_\sim = [x']_\sim$ allora

$$x \sim x' \Rightarrow \omega x \sim \omega x' \Rightarrow [\omega x]_\sim = [\omega x']_\sim$$

Definizione 2.6. Dati due insiemi X e Y con operazioni esterne sinistre μ, μ' sullo stesso insieme Ω, si chiama Ω-*omomorfismo* una funzione $f\colon X \longrightarrow Y$ tale che $\forall \omega \in \Omega$, $\forall x \in X$ si ha $f(\mu(\omega, x)) = \mu'(\omega, f(x))$.
Nel caso in cui l'operazione esterna sia un'azione destra allora f si dice Ω-*omomorfismo* se $\forall \omega \in \Omega$, $\forall x \in X$, $f(x^\omega) = f(x)^\omega$.

Osservazione. Gli Ω-omomorfismi da un Ω- insieme X a se stesso sono detti Ω-endomorfismi, con la composizione e l'identità formano il monoide $(End_\Omega(X), \circ, id_X)$.
Gli Ω-endomorfismi biiettivi si chiamano Ω-automorfimi e formano il gruppo $Aut_\Omega(X)$.

Inoltre UN Ω-omomorfismo iniettivo si dice Ω-epimorfismo, mentre quanto è suriettivo si dice Ω-monomorfismo.

Possiamo ora enunciare il seguente risultato.

Teorema 2.2.2 (Teorema fondamentale di omomorfismo)**.** *Siano X e Y due strutture algebriche dello stesso tipo con operazione esterna sullo stesso insieme Ω, sia $f\colon X \longrightarrow Y$ un omomorfismo. Allora:*

1. *l'immagine ImF è una Ω-sottostruttura di Y;*
2. *definiamo in X la relazione $\sim_f$ in questo modo: $\forall a, b \in X$, $a \sim_f b \Leftrightarrow f(a) = f(b)$. Allora $\sim_f$ è una Ω-congruenza in X;*
3. *la funzione $\pi\colon X \longrightarrow X/\sim_f$ tale che $\pi(x) = [x]$, dove $[x]$ è la classe di equivalenza di $x \in X$, è un Ω-epimorfismo;*
4. *la funzione $F\colon X/\sim_f \longrightarrow Y$, tale che $F([x]) = f(x)$, è ben definita, è un Ω-monomorfismo e $ImF = Imf$;*
5. *si ha $f = F \circ \pi$ e tale F è unica;*
6. *se f è un Ω-epimorfismo allora F è un Ω-isomorfismo.*

Dimostrazione. Innanzitutto definiamo le operazioni esterne μ e μ' sulle strutture X e Y:

$$\begin{aligned} \mu\colon \Omega \times X &\longrightarrow X & \qquad \mu'\colon \Omega \times Y &\longrightarrow Y \\ (\omega, x) &\longmapsto wx & (\omega, y) &\longmapsto wy \end{aligned}$$

1. Per provare che Imf è una sottostruttura di Y bisogna dimostrare che è chiusa rispetto all'operazione esterna μ', infatti $\forall \omega \in \Omega$, $\forall y \in Imf$, $\exists x \in X$ tale che si ha:
$$\mu'(\omega, y) = \mu'(\omega, f(x)) = f(\mu(\omega, x)) \in Y$$

2. Si deve dimostrare che $\forall a, b \in X$, $\forall \omega \in \Omega$ si ha $a \sim_f b \Rightarrow \omega a \sim_f \omega b$.
Se $a \sim_f b$ allora $f(a) = f(b)$, moltiplicando a sinistra per ω attraverso le azioni μ e μ' si ottiene
$$\mu'(\omega, f(a)) = \mu'(\omega, f(b)) \Rightarrow f(\mu(\omega, a)) = f(\mu(\omega, b)) \Rightarrow \omega a \sim_f \omega b$$

3. La proiezione π è un Ω-omomorfismo suriettivo, infatti $\forall \omega \in \Omega$, $\forall x \in X$ si ha
$$\pi(\omega x) = [\omega x]_{\sim_f} = \omega \, [x]_{\sim_f} = \omega \pi(x)$$
dove $[\omega x]_{\sim_f} = \omega \, [x]_{\sim_f}$ poichè $\sim_f$ è una Ω-congruenza.
Inoltre π è suriettiva in quanto $\forall \, [x]_{\sim_f} \in X/\sim_f$ si ha $\pi(x) = [x]_{\sim_f}$

4. La funzione F è ben definita in quanto $\forall x, x' \in X$ se $[x]_{\sim_f} = [x']_{\sim_f}$ allora $x \sim_f x'$ cioè $f(x) = f(x')$. In conclusione si ha
$$F([x]) = f(x) = f(x') = F([x])$$
Di più F è un Ω-omomorfismo, si ha:
$$F(\omega \, [x]) = F([\omega x]) = f(\omega x) = \omega f(x) = \omega F([x])$$
in quanto f è un Ω-omomorfismo.
Infine F è iniettivo poiché se $F([x]) = F([x'])$ cioè $f(x) = f(x')$ allora $x \sim_f x'$ cioè x, x' hanno la stessa classe di equivalenza.

5. Si ha $f = F \circ \pi$ infatti $(F \circ \pi)(x) = F(\pi(x)) = F([x]) = f(x)$
Inoltre tale F è unica: siano $F, F' \colon X/\sim_f \to Y$, supponiamo $F \circ \pi = f = F' \circ \pi$ allora
$$\begin{aligned} (F \circ \pi)(x) &= (F' \circ \pi)(x) \\ F(\pi(x)) &= F'(\pi(x)) \\ F([x]) &= F'([x]) \end{aligned}$$

6. Nel punto 4 abbiamo dimostrato che F è un Ω-monomorfimo. Inoltre F è iniettiva poichè composizione di funzioni iniettive perciò è un Ω- isomorfismo.

□

Definizione 2.7. Infine definiamo il *prodotto diretto* di Ω-insiemi X e Y come il prodotto $X \times Y$ i cui elementi sono del tipo: $(\omega x, \omega y) = \omega(x, y)$ dove $\omega \in \Omega$, $x \in X$, $y \in Y$.

Esempio 2.8. Sia X un insieme e sia $\Omega = \{f\}$ dove $f\colon X \to X$ è fissata. Allora si può definire l'azione esterna

$$\begin{aligned} \mu\colon \Omega \times X &\longrightarrow X \\ (f, x) &\longmapsto f(x) \end{aligned} \tag{2.1}$$

In questo modo si ha $\tau_f = f$.
Sia, per esempio, $X = \{1, 2, 3, 4, 5, 6\}$ e $f\colon X \to X$ tale che

x	1	2	3	3	5	6
$f(x)$	1	1	4	6	5	3

allora sono Ω-sottoinsiemi di X, oltre all'insieme $\emptyset$ e X stesso:

$$\{1, 2\}, \{3, 4, 5\}, \{1\}, \{5\}, \{1, 5\}, \{1, 3, 4, 6\}, \{4, 6\}, \{5, 6\}$$

mentre non lo sono:

$$\{2\}, \{3, 4\}, \{4, 6\}, \{5, 6\}$$

Sia $Y = \{1, 2\}$ allora il prodotto diretto $X \times Y$ ha 12 elementi. Ω agisce su Y come restrizione di f a Y:

y	1	2
$f(y)$	1	1

quindi si può definire l'azione $\mu\colon \Omega \times (X \times Y) \longrightarrow X \times Y$.
Per esempio $\mu(f, (4, 2)) = \mu(f(4), f(2)) = \mu(6, 1) = (3, 1)$

2.3 Condizioni di compatibilità

Nel caso in cui su Ω o su X sia presente un qualche tipo di struttura algebrica, si richiede che l'azione sia compatibile con tale struttura. In particolare si ha

1. Sia Ω un insieme e X un insieme con una struttura algebrica. Allora

   $$\mu\colon \Omega \times X \longrightarrow X$$

   definita come $\mu(\omega, x) = \tau_\omega(x)$, è un'azione sinistra se $\forall \omega \in \Omega$, $\tau_\omega \in End(X)$.

2. Sia Ω un insieme con una struttura algebrica e X un insieme. Allora μ è un'azione se all'interno di $X^X = \{f : X \longrightarrow X\}$ c'è una struttura H dello stesso tipo di Ω e la rappresentazione $\rho\colon \Omega \longrightarrow H$ è un omomorfismo.

3. Infine se entrambi gli insieme X e Ω hanno una struttra algebrica allora devono essere soddisfatte la 1) e la 2).

Nel prossimo capitolo vedremo alcuni esempi di azioni esterne tra insiemi sui quali è presente una struttura algebrica e ne analizzeremo la compatibilità. In questo modo ritroveremo gli esempi del capitolo 1, reinterpretati in chiave di operazioni esterne.

Capitolo 3

Esempi

Ora le nozioni introdotte nel primo capitolo possono essere reinterpretate a partire dallo studio fatto sulle operazioni esterne permettendoci di generalizzare il comportamento di alcune strutture algebriche e le nozioni ad esse associate.

3.1 Azione di un gruppo su un insieme

Definizione 3.1. Sia X un insieme e sia G un gruppo. Si definisce *azione sinistra* di G su X un'applicazione

$$\begin{aligned} \mu\colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

tale che:

i) $(gg')x = g(g'x), \forall g, g' \in G, x \in X$;

ii) $1_G x = x, \forall x \in X$.

In questo caso X si dice G-*insieme*.

Osservazione. L'applicazione $\mu\colon G \times X \longrightarrow X$ è un'azione sinistra se è compatibile con la struttura di gruppo di G quindi deve soddisfare la condizione 2 del capitolo 2.3. L'azione deve essere tale che la rappresentazione associata $\rho\colon G \longrightarrow X^X$ sia un omomorfismo di monoidi e che nel monoide delle funzioni da X a se stesso $(X^X, \circ, id)$ vi sia una struttura algebrica dello stesso tipo di G. La funzione

$$\begin{aligned} \rho\colon G &\longrightarrow X^X \\ g &\longmapsto \tau_g \end{aligned}$$

è un omomorfismo di monoidi infatti:

- $\forall a, b \in G$, $\forall x \in X$ si ha $\tau_{ab}(x) = (ab)x = a(bx) = \tau_a \circ \tau_b(x) \Rightarrow \tau_{ab} = \tau_a \circ \tau_b$ quindi $\forall a, b \in G$ vale $\rho(ab) = \tau_{ab} = \tau_a \circ \tau_b = \rho(a) \circ \rho(b)$

- $\rho(1_G) = id_X$

Inoltre $(\tau_a)^{-1} = \tau_{a^{-1}}$ quindi τ_a è biiettiva. Perciò $\forall a \in G$ si ha $\tau_a \in S_X \subseteq X^X$. Dunque la rappresentazione diventa $\rho\colon G \longrightarrow S_X$ ed è un omomorfismo di gruppi.

Inoltre $Im(\rho) \subseteq S_X$ e il nucleo è $Ker\rho = \{a \in G \,|\, \tau_a = id_X\}$ ossia
$a \in Ker\rho \Leftrightarrow \forall x \in G$, $\mu(a, x) = x$.

Viceversa dato un omomorfismo di monoidi, definito come sopra, l'applicazione $\mu\colon (g, x) \mapsto \tau_g(x)$ è un'azione di gruppo.

Definizione 3.2. Si definisce la relazione in X: $x \sim_G y$ se $\exists g \in G$ tale che $y = gx$. *È* una relazione di equivalenza. Infatti è

- riflessiva, $x \sim_G x$ poiché $x = 1_G x$

- simmetrica, se $x \sim_G y$ cioè $\exists g \in G$ tale che $y = gx$ allora $x = g^{-1}y$ perciò $y \sim_G x$

- transitiva, se $x \sim_G y$ e $y \sim_G z$ allora $\exists g \in G$ tale che $y = gx$ ed $\exists g' \in G$ tale che $z = g'y$ allora $z = g'(gx) = (g'g)x$ perciò $x \sim_G z$

La classe di equivalenza di $x \in X$ rispetto alla relazione $\sim_G$ si chiama *G-orbita* di $x \in X$: $Gx = \{gx \in X : g \in G\}$.
Osserviamo che le G-orbite sono G-sottoinsiemi, nel senso della definizione 2.4. Gli altri G-sottoinsiemi sono l'insieme $\emptyset$ e le unioni di G-orbite.

Definizione 3.3. Si chiama *stabilizzatore* di $x \in X$ in G l'insieme degli elementi che fissano x: $St_G(x) = \{g \in G : \mu(g, x) = x\}$, dove μ è l'azione sinistra del gruppo G sull'insieme X.

Proposizione 3.1.1. *Si ha che $St_G(x)$ è un sottogruppo di G e $Ker\rho = \bigcap_{x \in X} St_G(x)$.*

Dimostrazione. Per dimostrare che $St_G(x)$ è un sottogruppo è sufficiente provare:

- $1_G \in St_G(x)$ infatti $\mu(1_G, x) = 1_G x = x$;

- $a, b \in St_G(x) \Rightarrow ab \in St_G(x)$ infatti $\mu(ab, x) = (ab)x = a(bx) = ax = x$;

- $a \in St_G(x) \Rightarrow a^{-1} \in St_G(x)$ infatti per ipotesi $\mu(a, x) = ax = x$, è sufficiente moltiplicare a sinistra per a^{-1} e si ottiene $a^{-1}(ax) = a^{-1}x \Rightarrow x = a^{-1}x\mu(a^{-1}, x)$

Per provare che $Ker\rho = \bigcap_{x \in X} St_G(x)$ è sufficiente provare le due inclusioni: sia $a \in Ker\rho$ allora $\forall x \in X$ si ha $ax = x$ allora $a \in \bigcap_{x \in X} St_G(x)$.
Viceversa, se $a \in \bigcap_{x \in X} St_G(x)$ allora esiste almeno un $x \in X$ tale che $ax = x$ quindi di certo $a \in Ker\rho$. □

Definizione 3.4. L'azione μ si dice *transitiva* se $\forall x, x' \in X, \exists g \in G$ tale che $\mu(g, x) = x'$

Teorema 3.1.2. *Sia data un'azione del gruppo G sull'insieme X, sia $x \in X$. Allora:*

1. *L'insieme S dei laterali sinistri di $St_G(x)$ è equipotente a $[x]_G$.*
2. *Se G è finito si ha $|G| = |St_G(x)| \cdot |[x]_G|$. In particolare, se l'azione è transitiva si ha $|G| = |St_G(x)| \cdot |X|$.*

Dimostrazione. 1. Si definisce la relazione tra $S = \{gSt_G(x) \mid g \in G\}$ e $[x]_G$ come

$$f \colon gSt_G(x) \longmapsto gx$$

che è una funzione biiettiva infatti:

- $gx = hx \Leftrightarrow (h^{-1}g)x = x \Leftrightarrow h^{-1}g \in St_G(x) \Leftrightarrow g \in hSt_G(x) \Leftrightarrow gSt_G(x) = hSt_G(x)$ quindi f è iniettiva
- f è ovviamente suriettiva infatti $f(S) = [x]_G$.

2. Segue dal punto 1 e dal teorema di Lagrange secondo il quale l'ordine di un sottogruppo di un gruppo finito divide l'ordine del gruppo stesso.

□

3.1.1 L'azione del gruppo Γ delle isometrie sul piano euclideo

Un esempio di azione di un gruppo su un insieme è quello del gruppo Γ delle isometrie piane sul piano euclideo $\mathcal{P}$. Se consideriamo le figure del piano euclideo abbiamo che il gruppo Γ induce un'azione sulle figure piane.
Due figure piane $\mathfrak{F}_1$ e $\mathfrak{F}_2$ si dicono *isometriche* se esiste una isometria f tale che $f(\mathfrak{F}_1) = \mathfrak{F}_2$. In questo modo si ottiene una relazione di equivalenza nell'insieme delle figure piane, cioè dei sottoinsiemi di punti del piano, le cui classi di equivalenza sono dette *classi di isometria*. Per esempio la classe di isometria del quadrato è l'insieme dei quadrati con lati congruenti.
Inoltre per ogni figura $\mathfrak{F}$, possiamo considerare l'insieme $\{\alpha \in \Gamma | \alpha(\mathfrak{F}) = \mathfrak{F}\}$ che è sottogruppo di Γ detto *gruppo di simmetrie* di $\mathfrak{F}$.
Un Ω-sottoinsieme del piano $\mathcal{P}$ è unione di classi di isometria. Per esempio l'insieme dei poligoni è un Ω-sottoinsieme, come anche l'insieme dei punti, delle rette e delle coniche.

L'azione del gruppo Γ sul piano è transitiva sui punti e sulle rette in quanto $\forall P, P' \in \mathcal{P}$ esiste sempre una traslazione τ tale che $\tau(P) = P'$, basta prendere la traslazione di vettore v parallelo al segmento PP', nel verso che porta P in P' e di modulo pari alla lunghezza di PP'. Analago è il discorso per le rette: $\forall r, r' \in \mathcal{P}$, se non sono parallele è

sufficiente considerare la rotazione ρ di centro il punto di intersezione delle rette e ampiezza l'angolo α formato da esse; se invece $r//r'$ allora basta considerare la traslazione τ che porta r in r' di vettore perpendicolare a entrambe le rette e modulo pari alla loro distanza.

Per quanto riguarda le orbite si ha che l'orbita di un segmento è l'insieme dei segmenti ad esso congruenti; l'orbita di un angolo è l'insieme degli angoli ad esso congruenti e l'orbita di un poligono regolare con n lati è l'insieme dei poligoni regolari ad esso congruenti.

Lo stabilizzatore $G_{\mathfrak{F}}$ di una figura $\mathfrak{F}$ è detto *gruppo delle isometrie* di $\mathfrak{F}$, è costituito da tutte e sole le isometrie di Γ che trasformano l'insieme $\mathfrak{F}$ in sé.
Se definiamo una figura *limitata* come una figura piana $\mathfrak{F}$ che sia contenuta in un cerchio allora vale il seguente risultato che ne descrive lo stabilizzatore.

Teorema 3.1.3. *Sia $\mathfrak{F}$ una figura piana e $G_{\mathfrak{F}}$ il suo gruppo di isometrie, allora:*

1. *$G_{\mathfrak{F}}$ non contiene né traslazioni né antitraslazioni, a parte l'identità;*

2. *Tutte le rotazioni di $G_{\mathfrak{F}}$ hanno lo stesso centro per il quale passano tutti gli assi delle eventuali isometrie che appartengono a $G_{\mathfrak{F}}$.*

Dimostrazione. 1. Si procede per assurdo. Supponiamo che esista una traslazione $\tau \in G_{\mathfrak{F}}$, $\tau \neq id$ e sia d il modulo del vettore $v = v(\tau)$. Siano inoltre d il diametro di un cerchio che contiene $\mathfrak{F}$ e $P \in \mathfrak{F}$.
Ora $\forall n \in \mathbb{N}$, si pone $P_n = \tau^n(P)$ allora il segmento PP_n ha lunghezza pari a nd. Se $n > \frac{d}{d}$ allora $PP_n > d$. Quindi P_n non appartiene al cerchio che contiene $\mathfrak{F}$ dunque $P_n \notin \mathfrak{F}$ nonostante $P \in \mathfrak{F}$ e $\tau^n \in G_{\mathfrak{F}}$. Siamo allora arrivati all'assurdo.
Inoltre, poichè componendo due antitraslazioni si ottiene una traslazione, $G_{\mathfrak{F}}$ non contiene neanche antitraslazioni.

2. Ragioniamo ancora per assurdo. Supponiamo che esistano $\rho_1, \rho_2 \in G_{\mathfrak{F}}$, rotazioni con centri diversi. Poichè $G_{\mathfrak{F}}$ è un gruppo, $\rho_1 \circ \rho_2$ e $\rho_2 \circ \rho_1$ stanno ancora in $G_{\mathfrak{F}}$. Per il punto precedente, non possono essere traslazioni quindi sono rotazioni con la stessa ampiezza α e centri diversi. Ora poiché $\alpha + (-\alpha) = 0$, l'isometria $(\rho_2 \circ \rho_1) \circ (\rho_1 \circ \rho_2)^{-1} \in G_{\mathfrak{F}}$ è una traslazione, ma ciò è assurdo.
Infine si considerano in $G_{\mathfrak{F}}$ una rotazione ρ di centro O e una simmetria σ di asse $s \not\ni O$. Se si compongono, si ottiene l'isometria inversa $\rho \circ \sigma$ che è prodotto di tre simmetrie con assi che non passano per uno stesso punto e non sono tutti paralleli, perciò è un'antitraslazione. Ciò è assurdo, ancora per il punto precedente.

□

Esempio 3.5. Lo stabilizzatore di un quadrato è costituito da tutte le isometrie che lo trasformano in se stesso: le quattro rotazioni intorno al suo centro (punto di intersezione delle diagonali) di ampiezze $0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$ e le quattro simmetrie rispetto agli assi dei lati e alle diagonali.

In generale possiamo considerare un poligono regolare con n lati, è una figura limitata quindi il suo stabilizzatore è costituito dalle rotazioni ρ_k di ampiezza $\frac{2\pi k}{n}$, $0 \leq k < n$ e centro nel centro del poligono, e dalle simmetrie che hanno come assi le rette che congiungono O con i vertici del poligono o con i punti medi dei lati. Quindi il gruppo delle isometrie ha $2n$ elementi.

Se invece consideriamo una figura non limitata, il teorema precedente non vale.

Esempio 3.6. Si può determinare lo stabilizzatore di una retta studiando le rette unite da ciascuna isometria. Esso è costituito dalle traslazioni di vettore parallelo alla retta, dalle rotazioni di ampiezza π e centro un punto della retta, dalle simmetrie con assi la retta data o le sue perpendicolari e infine dalle antitraslazioni con asse la retta data.

3.2 Azione di un anello su un gruppo abeliano

Tra gli esempi di azione di una struttura algebrica Ω su un'altra struttura algebrica X consideriamo l'azione di un anello nel ruolo di Ω su un gruppo abeliano nel ruolo di X. In particolare analizzeremo gli spazi vettoriali e gli A-moduli.
Ora definiamo gli spazi vettoriali attraverso la nozione di operazione esterna:

Definizione 3.7. Siano K un campo e $(V, +)$ un gruppo abeliano.
Uno *spazio vettoriale* $V(K)$ è un gruppo abeliano V a cui è associata l'azione di K su V definita come

$$\begin{aligned} \mu\colon K \times V &\longrightarrow V \\ (k, v) &\longmapsto kv \end{aligned}$$

la quale associa a ogni elemento $k \in K$ e ad ogni elemento $v \in V$, l'elemento $kv \in V$. Tale azione deve soddisfare le seguenti condizioni analoghe a quelle introdotte nella definizione 1.3 del paragrafo 1.2:

i) $\forall h, k \in K$, $\forall v \in V$,

$$\begin{aligned} \mu((h+k), v) &= \mu(h, v) + \mu(k, v) \\ \mu(h, kv) &= \mu(hk, v) \end{aligned}$$

ii) $\forall k \in K, \forall v, w \in V,$

$$\mu(k, (v + w)) = \mu(k, v) + \mu(k, w)$$

iii) $\forall v \in V, \quad \mu(1_K, v) = v$

Ora utilizzando la notazione moltiplicativa dell'azione esterna μ possiamo reinterpretare la definizione di spazio vettoriale attraverso gli strumenti introdotti nel capitolo precedente e il seguente:

Lemma 3.2.1. *Sia $(V, +)$ un gruppo abeliano in notazione additiva. Allora l'insieme degli endomorfismi $End(V) = \{f | f : V \longrightarrow V$ omomorfimo$\}$ di V diventa un anello rispetto all'addizione punto per punto e alla composizione. Quest'ultima è distributiva rispetto all'addizione ed ha l'identita id_V come elemento neutro. Il suo gruppo delle unità è il gruppo $Aut(G)$.*

Dimostrazione. Per provare che $End(V)$ è un anello rispetto all'addizione punto per punto e alla composizione, bisogna verificare le proprietà di anello:

i) Dati $f, g \in End(V)$ definiamo l'addizione punto per punto: $\forall v \in V$

$$(f + g)(v) = f(v) + g(v)$$

Occorre provare che $f + g \in End(V)$:

$$\begin{aligned}((f + g))(v + w) &= (f)(v + w) + g(v + w) = \\ &= f(v) + f(w) + g(v) + g(w) = \\ &= (f + g)(v) + (f + g)(w)\end{aligned}$$

Inoltre $(End(V), +)$ è un gruppo abeliano con elemento neutro 0 infatti:

- vale la proprietà associativa dell'addizione:

$$\begin{aligned}((f + g) + h)(v) &= (f + g)(v) + h(v) = \\ &= f(v) + g(v) + h(v) = \\ &= f(v) + (g + h)(v) = \\ &= (f + (g + h))(v)\end{aligned}$$

- vale la proprietà commutativa:

$$\begin{aligned}(f + g)(v) &= f(v) + g(v) = \\ &= g(v) + f(v) = \\ &= (g + f)(v)\end{aligned}$$

- esiste un elemento neutro per l'addizione punto per punto tale che

$$(f+0)(v) = f(v) + 0(v) = f(v) + 0_V = f(v)$$

infatti basta prendere $0\colon v \mapsto 0_V$

- per ogni $f \in End(V)$, esiste $-f \in End(V)$ tale che

$$f + (-f) = 0$$

basta prendere $-f\colon v \mapsto -f(v)$

ii) Bisogna innanzitutto provare che $\forall v, w \in V$ e $\forall f, g \in End(V)$ si ha $f \circ g \in End(V)$, infatti

$$\begin{aligned}(f \circ g)(v+w) &= f(g(v+w)) = \\ &= f(g(v) + g(w)) = \\ &= f(g(v)) + f(g(w)) = \\ &= (f \circ g)(v) + (f \circ g)(w)\end{aligned}$$

Poi $(End(V), \circ)$ è un semigruppo infatti come è ben noto id_V è l'elemento neutro della composizione e vale la proprietà associativa:

$$\begin{aligned}((f \circ g) \circ h)(v) &= (f \circ g)(h(v)) = \\ &= f(g(h(v))) = \\ &= f((g \circ h)(v)) = \\ &= (f \circ (g \circ h))(v)\end{aligned}$$

Inoltre la composizione è distributiva rispetto all'addizione punto per punto infatti:

$$\begin{aligned}(f \circ (g+h))(v) &= f((g+h)(v)) = \\ &= f(g(v) + h(v)) = \\ &= f(g(v)) + f(h(v)) = \\ &= (f \circ g)(v) + (f \circ h)(v)\end{aligned}$$

Inoltre è sempre vero, anche per funzioni qualunque, che:

$$\begin{aligned}((f+g) \circ h)(v) &= (f+g)(h(v)) = \\ &= f(h(v)) + g(h(v)) = \\ &= (f \circ h)(v) + (g \circ h)(v)\end{aligned}$$

□

Questo Lemma permette di interpretare le tre proprietà, con le quali si è definito lo spazio vettoriale, nei termini delle condizioni di compatibilità. Le proprietà i) e iii) dicono che $\rho\colon K \longrightarrow End(V)$ è un omomorfismo di anelli mentre la proprietà ii) dice che $\tau_k \in End(V)$ dove τ_k è la funzione definita come $\tau_k(v) = \mu(k, v)$.
Osservazione. Se si considerano $\tau_k \in Aut(V)$ con $k \neq 0_K$ e l'omomorfismo ρ allora si ha: $Ker\,\{\tau_k\} = \{0_V\}$ e $Ker\,\{\rho\} = \{0_K\}$. In questo modo si può reinterpretare la legge di annullamento del prodotto negli spazi vettoriali. Infatti si ha:

$$kv = 0_V \Leftrightarrow k \in Ker\,\{\rho\} \vee v \in Ker\,\{\tau_k\} \Leftrightarrow k = 0_K \vee v = 0_V$$

Si può quindi definire una nozione fondamentale degli spazi vettoriali: la dimensione, cioè il numero di elementi di una qualsiasi base dello spazio vettoriale.

Definizione 3.8. Siano A un anello commutativo e G un gruppo abeliano. Si chiama A-*modulo* il gruppo abeliano $(G, +)$ insieme all'azione esterna

$$\begin{aligned} \mu\colon A \times G &\longrightarrow G \\ (a, g) &\longmapsto ag \end{aligned}$$

che ha le stesse proprietà definite sopra per lo spazio vettoriale.

Gli A-moduli sono una struttura algebrica che generalizza quella di spazio vettoriale. Per questo motivo si possono sottolineare alcune differenze: innanzitutto mentre nel caso degli spazi vettoriali, se l'operazione esterna è destra o sinistra si ottiene il medesimo risultato; nel caso degli A-moduli, se A è un anello non commutativo, si parla di A-moduli destri (rispettivamenti sinistri) se l'operazione esterna è destra (rispettivamente sinistra).
Inoltre la legge di annullamento del prodotto non vale negli A-moduli mentre vale negli spazi vettoriali; infine gli A-moduli non hanno lo stesso concetto di dimensione poiché non tutte le basi di un A-modulo hanno lo stesso numero di elementi.

Esempio 3.9. Si consideri il gruppo additivo $(A, +)$ di un anello A, esso può essere interpretato come A-modulo (destro o sinistro) rispetto all'anello stesso. Infatti si possono definire le azioni sinistra e destra:

$$\forall a \in A, \forall x \in A, \mu(a, x) = ax \quad (A\text{-modulo sinistro})$$

$$\forall a \in A, \forall x \in A, \mu(x, a) = xa \quad (A\text{-modulo destro})$$

che soddisfano ovviamente le proprietà i), ii), iii).

Se si considera un anello A come A-modulo su se stesso allora si può definire una sottostruttura detta A-sottogruppo.

Definizione 3.10. Sia A un anello commutativo. Si definiscono *A-sottomoduli* i sottogruppi I di $(A,+)$ tali che

$$\forall a \in A, \forall i \in I, \quad \text{si ha} \quad a \cdot i \in I$$

Si osservi che il sottogruppo I appena definito è un ideale di A, quindi gli ideali sono sottostrutture di A come A-modulo e non come anello.

Esempio 3.11. L'azione di $(\mathbb{Z},+,\cdot,1)$ su un gruppo abeliano $(V,+)$: Consideriamo ora l'insieme $\mathbb{Z}$ degli interi nel ruolo dell'anello A, allora la funzione

$$\begin{aligned} \mu\colon \mathbb{Z} \times V &\longrightarrow V \\ (n,v) &\longmapsto nv \end{aligned}$$

è un'azione per le proprietà delle potenze, infatti sono soddisfatte le condizioni di A-modulo. Gli $\mathbb{Z}$-sottomoduli sono tutti e soli i sottogruppi di $\mathbb{Z}$.
Inoltre vale la legge di annullamento del prodotto se e solo se ogni elemento $v \in V$, $v \neq 0_V$, ha periodo infinito. Per esempio, si consideri $(\mathbb{Z}_6,+)$ nel ruolo del gruppo V, sia $v = [1]_6$ allora $nv = [0]_6 \Leftrightarrow n$ è multiplo di 6, quindi non solo per $v = 0$ come accade negli spazi vettoriali.
Infine non tutte le basi hanno stessa dimensione, per esempio in $\mathbb{Z}_6$ si ha che $\{[1]_6\}$ e $\{[2]_6, [3]_6\}$sono basi ma non sono equipotenti.

3.3 Le azioni di un gruppo su se stesso

In questa sezione analizzeremo alcuni esempi di azione di un gruppo su se stesso: il coniugio e la moltiplicazione a sinistra. Attraverso la nozione di azione esterna si vogliono reinterpretare i concetti introdotti nel capitolo 1.4.

3.3.1 Il coniugio

L'azione di coniugio può essere interpretata come l'azione di un gruppo G su se stesso definendo l'operazione esterna

$$\begin{aligned} \mu\colon G \times G &\longrightarrow G \\ (a,x) &\longmapsto axa^{-1} \end{aligned}$$

In questo caso la funzione $C_a\colon G \longrightarrow G,\ C_a(x) = \mu(a,x) = axa^{-1}$, definita nel primo capitolo, è un endomorfismo; di più è un automorfismo di G. Infatti nel paragrafo 1.4 abbiamo dimostrato che $C_a(xy) = C_a(x)C_a(y)$ cioè l'applicazione C_a conserva l'operazione interna di G. Inoltre tale funzione è biiettiva: è iniettiva infatti vale

$$C_a(x) = C_a(y) \Leftrightarrow axa^{-1} = aya^{-1}$$

e moltiplicando a sinistra per a^{-1} e a destra per a si ottiene $x = y$.
Infine è suriettiva poiché l'immagine di C_a coincide con G.
Quindi abbiamo provato che è soddisfatta la condizione 1 del paragrafo 2.3.

Allora possiamo considerare $Aut(G) \subseteq G^G$ che ha la stessa struttura di gruppo di G, e la funzione

$$\begin{aligned} \rho = \rho_\mu \colon G &\longrightarrow Aut(G) \\ a &\longmapsto C_a \end{aligned}$$

La rappresentazione ρ è un omomorfismo di gruppi. Infatti

$$\rho(ab) = C_{ab} = C_a C_b = \rho(a)\rho(b)$$

In questo modo è soddisfatta anche la condizione 2 del paragrafo 2.3 quindi l'azione di coniugio è compatibile con la struttura di gruppo di G.

Inoltre il nucleo di ρ è il centro di G:

$$Ker\rho = Z(G) = \left\{a \in G | \forall x \in G,\, axa^{-1} = x\right\}$$

ed è un sottogruppo normale di G.

L'immagine di ρ, denotata con $Inn(G)$, è un sottogruppo del gruppo degli automorfismi $Aut(G)$.

Dimostrazione. Si vuole provare che $Im\rho = Inn(G) = \{\rho(a) \,|\, a \in G\} = \{C_a \,|\, a \in G\}$ è un sottogruppo:

- $id \in Inn(G)$ infatti basta considerare l'elemento C_1 tale che $C_1(x) = x$;
- $\forall a, b \in G$ sappiamo che $ab \in G$ quindi se $C_a, C_b \in Inn(G)$ allora pure $C_a C_b = C_{ab} \in Inn(G)$;
- infine $\forall a \in G$ si ha che $a^{-1} \in G$ quindi $(C_a)^{-1} = C_{a^{-1}} \in Inn(G)$

□

Quindi, per il teorema di omomorfismo di gruppi, si ha $G/Z(G) \cong Inn(G)$.

L'orbita di un elemento $x \in G$ prende il nome di classe di coniugio: $[x] = \{axa^{-1} \,:\, a \in G\}$; mentre lo stabilizzatore di x è il suo centralizzante:

$$Z(x) = St_G(x) = \left\{a \in G \,:\, axa^{-1} = x\right\} = \{a \in G \,:\, ax = xa\}$$

Consideriamo ora un generico sottogruppo H del gruppo G e un elemento $a \in G$. Possiamo trasferire l'azione all'insieme $\mathcal{P}(G)$ dei sottoinsiemi di G: l'insieme $aHa^{-1} = \{aha^{-1} : h \in H\} = C_a(H)$ è un sottogruppo di G, isomorfo ad H poiché $C_a \colon G \longrightarrow G$ è un isomorfismo.

Definizione 3.12. Due sottogruppi H e H' del gruppo G si dicono *coniugati* se $H' = aHa^{-1}$ per un qualche $a \in G$.

Quindi i G-sottoinsiemi sono le unioni delle classi di coniugio, se consideriamo l'azione del gruppo G su di sé allora i G-sottogruppi sono i sottogruppi unione delle classi di coniugio, detti normali in G; equivalentemente di ha la seguente:

Definizione 3.13. Un sottogruppo H del gruppo G si dice *normale*, $H \triangleleft G$, se $H = aHa^{-1} \quad \forall a \in G$.

In altre parole, G agisce su $\mathcal{P}(G)$ e trasforma l'insieme $L(G)$ dei sottogruppi di G in se stesso. Allora i sottogruppi normali sono oggetti che coincidono con i loro coniugati, quindi sono l'analogo degli elementi del centro $Z(G)$ nell'azione di G su G.

L'azione di coniugio può essere vista anche come azione dell'insieme sostegno del gruppo G su G, in questo caso basta verificare la condizione 2 del paragrafo 2.3 come abbiamo già fatto.

Analogamente, si può considerare l'insieme degli automorfismi $Aut(G)$ che agisce sul gruppo G definendo l'operazione esterna $\forall x \in G$, $\forall f \in Aut(G)$ come $\mu(x, f) = f(x)$. In questo caso gli $Aut(G)$-sottogruppi sono detti *sottogruppi caratteristici* di G; tra di essi troviamo $\{1_G\}$, G stesso e Z_G.

Infine se consideriamo $\Omega = End(G)$, gli $End(G)$-sottogruppi sono detti *pienamente invarianti*. Tra di essi, oltre a 1_G e G stesso, troviamo per esempio $G' =< \{a^{-1}b^{-1}ab | a, b \in G\} >$, detto *derivato* di G.

3.3.2 La moltiplicazione a sinistra

Definizione 3.14. Sia (G,+) un gruppo. Si definisce *moltiplicazione a sinistra* l'applicazione

$$\begin{aligned} \mu \colon G \times G &\longrightarrow G \\ (a, x) &\longmapsto ax \end{aligned}$$

dove si considera il gruppo G nel ruolo di Ω e l'insieme sostegno del gruppo nel ruolo di X rispetto alla definizione 3.1. Tale funzione è tale che $\forall a, b \in G$, $\forall x \in G$ si ha

i) $\mu(ab, x) = (ab)x = a(bx) = \mu(a, \mu(b, x))$

ii) $\mu(1_G, x) = 1_G x = x$

Questa applicazione è un'azione se soddisfa alle condizioni 1 e 2 del paragrafo 2.3. In primo luogo la funzione $\tau_a \colon G \to G$, definita da $\tau_a(x) = ax$ è biiettiva: è iniettiva poiché

$$\tau_a(x) = \tau_a(y) \Rightarrow ax = ay \Rightarrow x = y$$

ed è suriettiva infatti

$$\text{ogni } y \in G \text{ si può scrivere come } y = a(a^{-1}y) = \tau_a(\tau_{a^{-1}}(y))$$

In secondo luogo G^G contiene il gruppo simmetrico S_G e la rappresentazione $\rho \colon G \to S_G$, $\rho(a) = \tau_a$ è un omomorfismo di gruppi infatti $\forall a, b \in G$, $\forall x \in G$ si ha

$$\rho(a \cdot b)(x) = \tau_{a \cdot b}(x) = (a \cdot b)(x) = a \cdot (bx) = \tau_a \circ \tau_b(x) = \rho(a) \circ \rho(b)$$

L'azione μ è transitiva in quanto $\forall x, y \in G$, posto $a = yx^{-1}$, si ha l'uguaglianza $\mu(a, x) = ax = yx^{-1}x = y$; inoltre lo stabilizzatore di un qualsiasi elemento è il sottogruppo $\{1\}$.

Infine μ agisce anche sui laterali di un sottogruppo. Infatti sia H un sottogruppo del gruppo G, poniamo $xH = \{xh : h \in H\}$. Allora l'azione μ agisce su xH in questo modo:

$$\mu(g, xH) = (gx)H$$

In particolare lo stabilizzatore di un qualsiasi elemento di xH è $St_G(xH) = x^{-1}Hx$.

Dimostrazione. L'azione μ si trasferisce al laterale xH in questo modo:

$$\begin{aligned} \mu \colon G \times xH &\longrightarrow xH \\ (g, xh) &\longmapsto (gx)h \end{aligned}$$

infatti $\forall g \in G$, $\forall xh \in xH$ si ha $\mu(g, xh) = g(xh) = (gx)h \in xH$.
Inoltre se consideriamo $g \in G$, si ha

$$\begin{aligned} g \in St_G(xH) \Leftrightarrow g(xH) = xH \Leftrightarrow (x^{-1}gx)H = H \\ \Leftrightarrow \exists h \in H,\ x^{-1}gx = h \Leftrightarrow g = xhx^{-1} \in xHx^{-1} \end{aligned}$$

Pertanto $St_G(xH) = x^{-1}Hx$. □

Definizione 3.15. Si definisce *nocciolo* del sottogruppo H di G il nucleo della rappresentazione ρ, ossia

$$Ker\rho = \bigcap_{x \in G} St_G(xH) = \bigcap_{x \in G} x^{-1}Hx$$

In particolare, essendo $H = 1_G^{-1} H 1_G$, il nucleo di ρ è contenuto in H ed è un sottogruppo normale di G

Teorema 3.3.1 (*di Cayley*)**.** *Ogni gruppo finito G è isomorfo a un gruppo di permutazioni. Se G ha ordine n allora G è isomorfo a un sottogruppo del gruppo simmetrico S_n.*

Dimostrazione. Ad ogni $a \in G$ si associa $\tau_a \colon G \longrightarrow G$, definita da $\tau_a(x) = a \cdot x$, sappiamo già che questa funzione è biiettiva. Se consideriamo la rappresentazione $\rho \colon G \longrightarrow S_G$, definita da $\rho(a) = \tau_a$; è iniettiva infatti

$$\rho(a) = \rho(a') \quad \Rightarrow \quad \tau_a = \tau_{a'} \quad \Rightarrow \quad a = \tau_a(1_G) = \tau_{a'}(1_G) = a'$$

Inoltre $\forall a, a', x \in G$ si ha

$$\rho(a \cdot a')(x) = \tau_{a \cdot a'}(x) = (a \cdot a') \cdot x = a \cdot (a' \cdot x) = \tau_a(\tau_{a'}(x)) = \rho(a) \circ \rho(a')(x)$$

$$\Rightarrow \rho(a \cdot a') = \rho(a) \circ \rho(a')$$

Quindi ρ è un isomorfismo tra G e $\rho(S_G) \subseteq S_G$. Se $|G| = n$ allora $S_G \cong S_n$ dunque in S_n c'è un sottogruppo di ordine n e isomorfo a G. □

In questo modo abbiamo dimostrato che l'azione per moltiplicazione a sinistra (o a destra) è fedele in quanto è iniettiva.

Infine si può passare l'azione all'insieme $\mathcal{P}(G)$ dei sottoinsiemi di G: $\forall Y \subseteq G$, $\forall a \in G$ si ha che $\tau_a(Y)$ è equipotente a Y. Quindi le G-orbite in $\mathcal{P}(G)$ sono costituite da insiemi equipotenti (non tutti necessariamente nella stessa orbita).

Teorema 3.3.2 (*di Poincaré*)**.** *Se un gruppo G ha un sottogruppo H di indice finito n, ha anche un sottogruppo normale di indice finito, divisore di $n!$.*

Dimostrazione. G agisce sull'insieme $X = \{xH \mid x \in G\}$ come gruppo di permutazioni per moltiplicazione a sinistra, la sua immagine $\rho(G)$ è un sottogruppo di $S_X \cong S_n$ quindi $G/Ker\,\{\rho\} \cong \rho(G) \leq S_n$
Quindi $[G : Ker\,\{\rho\}]$ è finito e divisore di $|S_n| = n!$
Inoltre abbiamo visto che $Ker\rho = \bigcap_{x \in G} St_G(xH) = \bigcap_{x \in G} x^{-1} H x$ quindi $Ker\rho \subseteq H$. □

Conclusioni

Da quanto precede, dunque, ciò che hanno in comune gli esempi visti è l'azione di un insieme su un altro (o di una struttura su un'altra). Abbiamo osservato come alcune delle nozioni generali sulle azioni, per esempio gli Ω-sottoinsiemi, le Ω-congruenze, gli Ω-omomorfismi e gli Ω-prodotti diretti, acquistano un significato particolare in alcune delle situazioni analizzate, mentre in altre no.

Per esempio gli Ω-omomorfismi nel caso degli spazi vettoriali sono le importanti applicazioni lineari; nel caso dell'azione di un gruppo su un insieme, invece, hanno minore importanza.

Gli Ω-sottoinsiemi, al contrario, sono importanti per quasi tutti gli esempi visti. Sono Ω-sottoinsiemi i sottospazi di uno spazio vettoriale, gli ideali di un A-modulo, i sottogruppi normali cioè le unioni di classi di coniugio, le G-orbite dell'azione di un gruppo su se stesso e le loro unioni.

Le Ω-congruenze poi sono importanti nel caso degli spazi vettoriali e dell'azione di un insieme Ω su un gruppo G. Di quest'ultimo caso abbiamo visto solo qualche esempio: l'azione di coniugio (azione di un gruppo su se stesso) reinterpretata come azione dell'insieme sostegno del gruppo G sul gruppo G stesso. Inoltre abbiamo studiato l'insieme degli endomorfismi $End(G)$, o degli automorfismi $Aut(G)$, che agisce sul gruppo G di cui abbiamo visto gli $End(G)$-sottogruppi e gli $Aut(G)$-sottogruppi.

Infine gli Ω-prodotti diretti non sono stati approfonditi ma possiamo osservare che hanno importanza nel caso dell'azione di un anello su un gruppo quindi per gli spazi vettoriali e gli A-moduli.

L'algebra, come sempre, ci dà modo di generalizzare e unificare le nozioni studiate, ci permette di interpretare gli spazi vettoriali, gli A-moduli, le isometrie del piano, la moltiplicazione a sinistra e il coniugio come insiemi (o strutture algebriche) che agiscono su un altro insieme (o struttura algebrica) tramite un'applicazione con ben definite caratteristiche e proprietà.

Bibliografia

[1] M. Artin, *Algebra*, Bollati Boringhieri, 1997

[2] H. Freudenthal, *La matematica nella scienza e nella vita*, Il Saggiatore, 1967

[3] D. J. Robinson, *A course in the theory of groups*, Springer, 1996

[4] S. Rose, *A course on Group Theory*, Cambridge University Press, 1978

[5] E. Sernesi, *Geomtria 1*, Bollati Boringhieri, 1989

[6] J. L. Verardi, *Dispense del corso di Algebra Superiore*, A.A. 2006/2007

[7] A. Vistoli, *Note di algebra*, Bologna, 1993/94

Ringraziamenti

Un caloroso ringraziamento va al relatore Prof. Libero Verardi per l'attenzione, la pazienza e l'entusiasmo con cui mi ha seguito negli ultimi due mesi. La sua passione per la matematica, e in particolare per l'algebra, mi ha contagiato ed ha riaccesso il mio amore per questa materia e il suo insegnamento.
Devo un grande grazie agli amici di sempre, gli zolesi, perché a modo loro mi sono sempre stati vicini.
Ringrazio i miei compagni di università: Simo e la Giuggi per il loro conforto, le parole gentili e l'ottimismo che mi hanno trasmesso in questi anni, anche ora che siamo così lontani. Un grazie a Riki, sempre disponibile per un caffè e una chiacchierata.
Il ringraziamento più importante va al mio mental coach, il mio Luca. Mi è stato vicino quando ne avevo bisogno, mi ha supportato e sopportato negli ultimi tre anni. Più di tutto mi ha aiutato a lottare e conquistare ciò che desidero. Oggi per me non è solo un traguardo, ma l'inizio della nostra avventura.
Infine ringrazio la mia famiglia: la mia mamma, la nonna Pola e Uber, perché ci sono. Sempre.